# Chapter 18
# Internal Marketing Cybersecurity-Conscious Culture

**Gordon Bowen**
*Northumbria University, London, UK*

**Atul Sethi**
*Ulster University, London, UK*

## ABSTRACT

*The chapter is putting forward the idea that internal marketing is a tool of which there are many to embed a culture to combat cybersecurity threats. This conceptual paper is suggesting that cybersecurity threats are multi-facet and although internal marketing is a major contributing factor in reducing the threats, other factors are in play. The shape of the organisation (i.e., bureaucratic or organic) has an important bearing on the implementation of a marketing-oriented culture, including that of internal marketing and, thus, the success of a cybersecurity-conscious organisational culture. Another significant factor in creating a cybersecurity-conscious organisational culture is the management willingness to empower and employees and their willingness to accept the responsibility to make decisions and be accountable, which requires acceptance of the authority.*

## INTRODUCTION

Cybercrime will cost societies $6 trillion annually by 2019, which is twice the cost of what was paid in 2015. Escalating at this rate requires serious action to be taken by organisations, society, and governments. To combat cybercrime currently, $1 trillion is spent on cybersecurity (radiusits.com). The focus of this paper is on the internal environment of the firm from the perspective of internal marketing to combat the internal threat of cybercrime and improve awareness of cybersecurity by using an internal marketing lenses.

DOI: 10.4018/978-1-6684-3698-1.ch018

The organisational landscape has a bearing on the effectiveness of combatting cybersecurity issues (Nye, 2017). Cybersecurity combines "public good" attributes, frequently associated with governmental responsibilities for private market goods and services, and private organisations with non-market, non-governmental resources, and information sharing. Management of governmental responsibilities requires a robust governance structure (Kuerbis & Badiei, 466, 2017). The paper suggests that not only governments and nations have responsibility for cybersecurity, but the organisation and employees have ownership of the governance structures internally to mitigate the effects of cybercrime. Furthermore, some of the responsibilities of government need to be cascaded down to organisations to gain the organisational commitment necessary for organisations to defend their organisation and employees against cybercrime. Shackelford & Kastelic, (2015) suggest there is a growing agreement that nations need to take responsibility for enhancing cybersecurity. Ultimately, governments and nations will require to engage organisations in cybersecurity, and organisations must shoulder more of the burden of cybersecurity. To ensure firms are ready to engage with the responsibilities of governance and activities related to cybersecurity, the paper contends that an internal marketing approach is necessary, because cybersecurity is everyone's responsibility, and employee responsibility is a key driver to guarantee cybersecurity safeguarding of the organisation.

## THEORETICAL CONCEPTS

### Determinants of internal marketing

"Market orientation", "market-driven" or "customer orientation" are used interchangeably and have a component of internal marketing orientation (IMO) (Naude´, Desai & Murphy,:1205, 2003). There is no agreed definition of the internal marketing construct (Rafiq & Ahmad, 2000). The use of marketing approaches within the organisation to create and publicise overall corporate values is an integral part of internal marketing (Hogg & Carter, 2000). The paper is positioning IMO as an important factor to embed a positive factor to embed employee engagement in detecting and preventing cybercrime within the organisation.

Schneider, (1990) and James el (1979) consider the perception of organisational climate is based on "person" and "situation" variables. Person x situation = perception of organisational climate. The Table 1 identifies the variables (Person and Situational) and the perception of the organisation (situation x person) (see *Table 1)*.

Naude´, Desai & Murphy, (2003) develop the following hypotheses for the variables in Table 1:

1. IMO will vary by age – younger age groups and generations will have stronger attitudes and transfer the expectations to the organisation. A significant factor is an age as a determinant of IMO. This implies that younger people's attitudes would need moulding to the organisational cybersecurity policies and procedures to ensure consistency in the operational requirements.
2. IMO results from males (gender) will be positive. The results bear this out that there is a positive outcome between males and IMO. Females tend to be more critical than men. This particular variable is not significant as a determinant of IMO.